Upgrade Guide

Forcepoint DLP

v8.6.x

Published 2018

Last modified 30-Nov-2018

Contents

1 Preparing to Upgrade to Forcepoint DLP v8.6

The existing Forcepoint DLP or TRITON AP-DATA installation must be at one of the following versions to upgrade to version 8.6.0:

- 8.5.2
- 8.5.1
- 8.5.0
- 8.4.x
- 8.3.x
- 8.2.x

If you have an earlier version, you will need to upgrade to version 8.2 first before beginning your upgrade to 8.6.

The existing data security solution must be at least version 8.2.x to upgrade directly to Forcepoint DLP version 8.6. Those currently using an earlier version must perform interim steps, as shown in the table below:

Current version	Step 1	Step 2	Step 3	Step 4
7.6.x	Upgrade to 7.7.2	Upgrade to 7.8.4	Upgrade to 8.4.x	Upgrade to 8.6
7.7.x	Upgrade to 7.8.4	Upgrade to 8.4.x	Upgrade to 8.6	
7.8.1–7.8.3	Upgrade to 7.8.4	Upgrade to 8.4.x	Upgrade to 8.6	
7.8.4	Upgrade to 8.4.x	Upgrade to 8.6		
8.0.x, 8.1.x	Upgrade to 8.3.x	Upgrade to 8.6		
8.2.x–8.5.x	Upgrade to 8.6			

Step-by-step guides to upgrading to earlier versions are available:

- Upgrading to Forcepoint DLP v8.5
- Upgrading to TRITON AP-DATA from v7.7.x - 7.8.x
- Upgrading to TRITON AP-DATA from v7.6.x - 7.8.x

To get started, see:

1. *Prepare for upgrade*
2. *Download and launch the installer*

Prepare for upgrade

To ensure a successful upgrade:

1. Unless instructed otherwise by Forcepoint Technical Support, make sure the system is functional prior to upgrade.
2. Verify that the starting version is 8.2.x, 8.3.x, 8.4.x, or 8.5.x.
3. Perform a full backup of the system (including both product and infrastructure backups, as described in the appropriate version of the Backup and Restore FAQ).
4. If fingerprinting tasks are running, stop the fingerprinting and disable the scheduler.
5. Route all traffic away from the system.
6. Ensure that any supplemental fingerprint repositories are fully synchronized with the primary repository. Check for synchronization in the system log.
7. Log on to the management console to make sure all settings are deployed successfully. (If the **Deploy** button is highlighted, click it.)
8. If the existing deployment includes Forcepoint-supplied custom file types, change the name of the following configuration files as follows:
   a. Navigate to the **\policies_store\custom_policies\config_files** subdirectory under the installation directory for your product.
   b. Rename “extractor.config.xml” to **custom_extractor.config.xml**.
   c. Rename “extractorlinux.config.xml” to **custom_extractorlinux.config.xml**.

   The file names are case-sensitive.
9. If administrators have removed applications from the product’s predefined endpoint application groups, make a list of the changes. Application groups are restored after upgrade, the applications will need to be removed again. Custom user-defined groups are unaffected.
10. Disable User Account Control (UAC) and Data Execution Prevention (DEP) settings, and make sure that no Software Restriction Policies will block the installation. The UAC settings can be re-enabled following the upgrade.

The speed and success of the upgrade process are affected by many factors, including:

- Number of online incidents
- Size of the forensics folder
- Number of policies or rules in use
- User directory import size
- Whether GPO restrictions are enforced on the server in domain membership scenarios

- Hardware specification

Download and launch the installer

The Forcepoint Security Installer (ForcepointDLP86Setup.exe) is used to upgrade the management server and other Windows-based servers.

The management server is always upgraded first.

To download the installer onto the management server machine:

1. Navigate to support.forcepoint.com and click the **My Account** link.
2. Log in, click **Downloads** in the menu bar at the top of the page, then click the **All Downloads** link.
3. Under **Data Security > Forcepoint DLP**, click the **8.6** link.
4. Select **Forcepoint DLP** in the list of installers.
5. On the Product Installer page, click the **Download** link near the bottom of the page.
6. When the installer has downloaded successfully, double-click the file to launch the installer.

   It may take several minutes for the installer to unpack files and launch. This is expected behavior.

The installation package detects that earlier versions of the product are installed, and automatically starts a series of wizards.

After upgrade, the system has the same configuration as before the upgrade. The upgrade process does not allow the option to change configuration or settings.

2 Upgrading Forcepoint DLP

Perform the upgrade steps in the order described.

Start the upgrade process by upgrading the management server. This is critical, because if supplemental servers or agents are upgraded before the management server, they stop communicating. When the management server is upgraded first, it continues communicating with the components until they are upgraded.

1. *Upgrade the management infrastructure*, page 5.
2. *Upgrade data security components on the management server*, page 6.
3. *Complete post-upgrade steps on the management server*, page 8.
4. After upgrading the management server, upgrade supplemental servers and any other server components:
   - *Upgrade supplemental servers and Windows-based agents*, page 8.
   - *Upgrade protectors and mobile agents*, page 9.
   - *Upgrade the Forcepoint DLP Protector software*, page 10.
   - *Upgrade the analytics engine*, page 11.
5. After upgrading the management server and other server components, it is essential to deploy changes (see *Deploy settings*, page 12).
6. Next, in deployments that include endpoint software, *Upgrade endpoint client software*, page 12.
7. If you are using Dynamic Data Protection (Endpoint DLP and UEBA), you need to download the RAP User Manager tool to enable users for Dynamic Data Protection on a DLP system. See the DDP Getting Started Guide for more information.
8. If you upgrade from version 8.5.2 to 8.6, it is necessary to enable and reconfigure your Risk-Adaptive Protection settings in the Forcepoint Security Manager after the upgrade is complete. See *Reconfigure Risk-Adaptive Protection in Forcepoint DLP*, page 14.

Upgrade the management infrastructure

The Forcepoint Infrastructure provides basic framework for all of the components that make up management server. This framework includes a central settings database that stores shared configuration (like administrator directory and account information) for all management modules, as well as other internal shared services.

The infrastructure upgrade wizard contains the following screens.

Wizard Screen	Fields
Welcome	Initiates the wizard. 1. Click **Next** to begin the upgrade process. The system checks disk space requirements. 2. When prompted, click **Next** to launch the installation wizard.
Pre-Installation Summary	Shows information about the upgrade, including: ● The destination folder for the installation files ● The name of the SQL Server machine and the user name of an authorized database administrator ● The IP address of the management server and its administrator credentials Click **Next** to accept the properties.
Installation	Shows upgrade progress. The system stops processes, copies new files, updates component registration, removes unused files, and more. A popup message appears at this stage, warning that all modules must be upgraded. This popup may be hidden behind the main installer window, so if the upgrade process appears to freeze, locate the hidden popup by moving the main installer window, then click **OK** to proceed. In addition, if a Data Task Scheduler window opens, the installer offers the option to stop the Work Scheduler service, or continue running the installer and reboot at the end. Reboot is the recommended approach.
Summary	Provides an overview of what has been upgraded, including: ● The destination folder for the installation files ● The name of the SQL Server machine and the user name of an authorized database administrator ● The IP address of the management server and its administrator credentials Click **Finish** to complete the upgrade for this module. Restart the machine if prompted.

Upgrade data security components on the management server

Before running the Forcepoint DLP upgrade wizard, the installer validates system requirements to ensure the upgrade will be successful.

The pre-upgrade check validates hardware requirements, credentials for the SQL Server management database, endpoint security certificates, manager configuration, administrator upgrade permissions, and the database structure. As it proceeds, it reports whether a step succeeded or failed, or it shows a warning.

- If there is a failure, the upgrade stops. For details, see **\TRITON-PreUpgrade-SystemTests.log** in the product's installation directory.
- If there are only warnings, the installer offers the option to continue the upgrade. Continuing without repairing the issues may cause unexpected behavior, but should not a critical impact.
- If the pre-upgrade check succeeds, or if the administrator continues after viewing warnings, the Forcepoint DLP wizard is launched, followed by wizards for each installed component.

The Forcepoint DLP upgrade wizard contains the following screens.

Wizard Screen	Fields
Welcome	Initial Forcepoint DLP installation wizard launch page. The system checks the disk space on the machine. When prompted, click **Next** to launch the installation wizard.
Configuration	Step through the screens configured during the previous product installation, including Fingerprinting Database, Temporary File Location, and Local Administrator. Click **Next** on each to retain the existing settings.
Installation Confirmation	Review the settings on the Installation Confirmation screen and click **Install** to continue the upgrade.
Installation	Shows the progress of the installation. The system stops processes, checks ports, copies new files, updates component registration, removes unused files, and more. In certain circumstances, an internal SQL error may appear. If this occurs, do not click OK until the issue has been resolved with Forcepoint Technical Support. Continuing without resolving the issue can cause problems with the reporting database.
Summary	Summarizes the upgrade configuration. 1. Click **Done**. A prompt about updating predefined policies and content classifiers appears. 2. Click **OK** to install the updates. The status of the updates is displayed, including the items being updated and details such as how many policies are updated, deleted, or added. 3. Click **Close** when the updates are complete. Restart the computer, if prompted.

Complete post-upgrade steps on the management server

After the upgrade process has completed successfully:

1. Log on to the management server machine with Administrator permissions.
2. To re-register all other components to the management server, run the appropriate installer on each host machine (see *Upgrade supplemental servers and Windows-based agents*, page 8).
3. Log into the Forcepoint Security Manager.
4. If applications were removed from the predefined endpoint application groups prior to upgrade, go to the **Main > Resources > Endpoint Application Groups** page and remove them again.
5. After upgrading all components, click **Deploy** in the Security Manager.

Upgrade supplemental servers and Windows-based agents

To upgrade a supplemental Forcepoint DLP server, or a Windows-based standalone agent, to v8.6:

1. Launch the Forcepoint Security Installer, **ForcepointDLP86Setup.exe**. The software is detected and the upgrade wizard appears.
2. Click **Next** until the wizard is completed.

   Forcepoint DLP components found on this machine from a supported previous version are upgraded.
3. Finishing the upgrade process requires deploying changes in the Forcepoint Security Manager. As a best practice, finish upgrading all components, then log into the Forcepoint Security Manager and deploy all of the changes at once.
4. Wait 30 minutes before routing traffic though the upgraded system.

   This allows the upgraded server time to download the information necessary for resolving source and destination resources such as people, computers, and printers. Routing traffic through the system before this is complete may cause:

   - Potential false positives and negatives
   - File-system discovery problems, where the discovery starts but immediately fails

Upgrade protectors and mobile agents

Version 8.6 of the protector includes CentOS 7. Protectors can be upgraded from v8.2.5 and later to v8.6, but not from earlier versions. Versions prior to v8.2.5 are built on Cent OS 5.

For protector versions prior to v8.2.5, there are two options:

- Re-image the protector from scratch. See *Reinstalling the protector or mobile agent*, page 9.
- Retain the existing installation.

  The protector and mobile agent are forward compatible, so older versions can still take advantage of v8.5 management, analytic, and endpoint features.

> **Important**
>
> If the protector is migrated to new hardware, be sure to keep the original IP address and hostname in order to retain settings and information from the original machine.
>
> When the protector is assigned a new IP address, the protector's settings are restored to the default when it registers with the management server. In this situation, manually delete the protector with the original IP address from the System Modules page of the Security Manager.

To upgrade a v8.2.5 or later protector or mobile agent to v8.5, see *Preparing to upgrade the protector or mobile agent*, page 10.

Reinstalling the protector or mobile agent

Perform these steps if you have an existing protector or mobile agent instance at a version prior to v8.2.5.

1. Back up any customizations to the protector, because the system will be wiped. This includes things like changes to the postfix configuration (/etc/postfix), network interface settings, and security certificates.

   Management configuration, such as policy and agent settings, are recovered when the new module is deployed.
2. Install the protector or mobile agent software as described in the Forcepoint DLP Installation Guide.
3. Restore any customizations.
4. Wait 30 minutes before routing traffic though the new system. It takes time to download the information necessary for resolving source and destination resources such as people, computers, and printers. Routing traffic through the system before this is complete may result in false positives and negatives.

Preparing to upgrade the protector or mobile agent

Use these steps if the protector or mobile agent is at v8.2.5 or later.

To download the upgrade script on the protector or mobile agent machine:

1. Navigate to support.forcepoint.com and click the **My Account** link.
2. Log in, then click **Downloads** in the menu bar at the top of the page.
3. Under Data Security > Forcepoint DLP, click the **8.6.0** link.
4. Select **Forcepoint DLP Appliance Upgrade Script from 8.2.5, 8.3, 8.4, or 8.5.x to 8.6** in the list of installers.
5. On the Product Installer page, click the **Download** link near the bottom of the page.
6. When the download is complete, unzip the **ProtectorMobileUpdate86.zip** file.
7. Copy the resulting file, **protector-update-8.6.x-yyyy**, to directory **/tmp** directory.

   Here, *x-yyyy* is the latest version and build number, such as 8.6.0-3456.

Upgrading the protector or mobile agent

To run the upgrade script:

1. Enter the following command:

   ```
   chmod +x /tmp/protector-update-8.6.x-yyyy
   ```
2. Enter the following command:

   ```
   bash /tmp/protector-update-8.6.x-yyyy
   ```
3. Answer **Y** on the “Are you sure?” question, and complete the wizard, accepting the defaults.
4. Restart the protector or mobile agent machine when the wizard completes.
5. Deploy changes to complete the upgrade process. See *Deploy settings*, page 12.
6. Wait 30 minutes before routing traffic though the new system. It takes time for it to download the information necessary for resolving source and destination resources such as people, computers, and printers. Routing traffic through the system before this is complete may result in false positives and negatives.

Upgrade the Forcepoint DLP Protector software

If your deployment includes the Forcepoint DLP Protector software package, the upgrade process differs slightly from that described in *Upgrade protectors and mobile agents*, page 9. Use the following steps to upgrade the Protector software package.

1. To download the software protector installer:

   a. Navigate to support.forcepoint.com and click the **My Account** link.

   b. Log in, then click **Downloads** in the menu bar at the top of the page.

   c. Under Data Security > Forcepoint DLP, click the **8.6.0** link.
   d. Select **Forcepoint DLP Network appliance software package (Protector)** in the list of installers.
2. Log in to the installation machine as **root** and copy the installation file into the Protector's /tmp directory.
3. Run the following command:

   ```
   chmod +x /tmp/ForcepointDLP86ApplianceSoftwarePackage
   ```
4. Execute **ForcepointDLP86ApplianceSoftwarePackage**.
5. Complete the wizard.
6. Restart the Protector.

Upgrade the analytics engine

To upgrade the analytics engine to v8.6:

1. To download the analytics engine installer (AnalyticsEngine86):
   a. Navigate to support.forcepoint.com and click the **My Account** link.
   b. Log in, then click **Downloads** in the menu bar at the top of the page.
   c. Under Data Security > Forcepoint DLP, click the **8.6.0** link.
   d. Select **Forcepoint DLP Analytics Engine software package** in the list of installers.
   e. On the Product Installer page, click the **Download** link.
2. Log in to the installation machine as **root** and copy the installation file to the current working directory.

   Make sure the installation file has execution privileges.
3. To run the installer, enter:

   ```
   ./AnalyticsEngine86
   ```

   The installer recognizes that a previous version of the analytics engine exists and initiates the upgrade process.

   - If a “permission denied” error appears, run the following command:

     ```
     chmod +x AnalyticsEngine86
     ```
   - If a “missing packages” error appears, follow the instructions in the message to install the required packages using yum.

     After installing the required packages, run the **.AnalyticsEngine86** command again.

Deploy settings

After upgrading all servers, agents, and appliances to Forcepoint DLP v8.6, deploy changes in the Forcepoint Security Manager. Endpoints do not require a separate deploy step.

1. Log into the Data Security module of the Forcepoint Security Manager.
2. When prompted to update policies, follow the on-screen instructions.

   Depending on the number of existing policies, this can take up to an hour. During this time, do not restart the server or any of the services.
3. Click **Deploy**.

Upgrade endpoint client software

- Version 8.1.0 and later Windows endpoint clients may be directly upgraded to v8.6.
- Version 8.3.0 and later Mac endpoint clients may be directly upgraded to v8.6.
- The v8.6 Forcepoint DLP server components can be used with endpoint clients at versions 8.1 and later.
- Endpoint client software maintains compatibility with older endpoint server versions, when possible. Endpoint clients can generally be upgraded, even if the endpoint server is not upgraded.

To upgrade existing on-premises version of the endpoint client:

1. Make sure that a supported management server version is installed and functioning.
2. Make a backup copy of the Endpoint Package Builder executable file found in the following location:

   ```
   C:\Program Files (x86)\Websense\Data Security\client
   ```
3. Navigate to support.forcepoint.com and click the **My Account** link.
4. Log in, click **Downloads** in the menu bar at the top of the page, then click the **All Downloads** link.
5. Under Endpoint Security > Forcepoint DLP Endpoint, click the **8.6** link.
6. Select the latest endpoint installer in the list.
7. On the Product Installer page, click the **Download** link.
8. Unzip the downloaded file in the Endpoint Package Builder folder referred to in step 2.

   Four files are placed in the directory: WebsenseEndpointPackageBuilder.exe, WebsenseEPClassifier.pkg.zip, EPA.msi, and EPA64.msi.

   - The exe file is for building software package to install on endpoint client machines.

- The zip file is a DLP endpoint classifier exclusively for Mac endpoints running Forcepoint DLP Endpoint.
- The EPA.msi file is the endpoint classifier for Win32 endpoints.
- The EPA64.msi file is the endpoint classifier for Win64 endpoints.

9. For Forcepoint DLP Endpoint software for Mac clients:

   a. Back up the **WebsenseEPClassifier.pkg.zip** file in the following folder:

      `C:\Program Files (x86)\Websense\Data Security\client\OS X`

   b. Copy the new **WebsenseEPClassifier.pkg.zip** from the folder in step 3 and place it into the \OS X folder.

      Do not unzip this file.

10. For Forcepoint DLP Endpoint software for Win32 clients:

    a. Back up the file **EPA.msi** in the following folder:

       `C:\Program Files (x86)\Websense\Data Security\client`

    b. Copy the new **EPA.msi** file to:

       `C:\Program Files (x86)\Websense\Data Security\client`

11. For Forcepoint DLP Endpoint software for Win64 clients:

    a. Back up the file **EPA64.msi** in the following folder:

       `C:\Program Files (x86)\Websense\Data Security\client`

    b. Copy the new **EPA64.msi** from the folder in step 2 and place it into

       `C:\Program Files (x86)\Websense\Data Security\client`

12. Run **WebsenseEndpointPackageBuilder.exe** to generate a new endpoint client installation package.
13. Deploy the v8.6 installation package to each endpoint client using one of the methods described in the Installation and Deployment Guide for Endpoint Solutions.
14. Restart the endpoint client machine after installation is complete.

After upgrading the endpoint software

The system provides both name and serial number for each endpoint device, as in “SanDisk Cruzer Blade; 4C530103131102119495”.

An easy way to maintain compatibility with previous releases is to add an asterisk (*) to the end of each device name listed in the Security Manager. For example, change “SanDisk Cruzer Blade” to “SanDisk Cruzer Blade*”.

Without this change, rules related to the existing endpoint devices may not monitor or enforce the removable media channel as expected. Only exact matches generate an incident.

Reconfigure Risk-Adaptive Protection in Forcepoint DLP

If you upgrade from version 8.5.2 to 8.6, it is necessary to reconfigure your Risk-Adaptive Protection settings after the upgrade is complete. Use the following steps for the configuration.

1. Log on to the Data Security module of the Forcepoint Security Manager.
2. Go to the **General > Services > Risk-Adaptive Protection** page.
3. Mark the check box **Enable Risk-Adaptive Protection**.
4. Enter the Forcepoint UEBA host name and port.
5. Click **Test Connection** to verify the connectivity with Forcepoint UEBA.
6. Click **OK** to save your settings.
7. Click **Deploy**.
8. Restart Windows service: **Websense Data Security Batch Server**.